

What is claimed is:

1 1. An apparatus authentication system which comprises
2 a server apparatus and a client apparatus which perform a mutual
3 authentication when a content is transmitted from the server
4 apparatus to the client apparatus for use therein, wherein
5 the client apparatus includes:
6 a receiving unit operable to receive challenge data from
7 the server apparatus;
8 a signature generating unit operable to generate signature
9 data based on the received challenge data and a first password;
10 and
11 a transmitting unit operable to transmit the generated
12 signature data, and
13 the server apparatus includes:
14 a challenge data transmitting unit operable to generate
15 and transmit the challenge data;
16 a holding unit operable to hold a second password in
17 advance;
18 a receiving unit operable to receive the signature data
19 from the client apparatus;
20 an authentication unit operable to perform an
21 authentication of the received signature data based on the
22 challenge data and the second password; and
23 a content transmitting unit operable to, if the
24 authentication results in success, transmit an encrypted content
25 to the client apparatus, the encrypted content having been
26 encrypted in such a manner that the encrypted content can be
27 decrypted by the client apparatus.

1 2. A server apparatus for transmitting a content to a
2 client apparatus, comprising:

3 a holding unit operable to hold a registered password;
4 a challenge data transmitting unit operable to generate
5 and transmit challenge data;

6 a receiving unit operable to receive, from the client
7 apparatus, signature data that has been generated based on a
8 password and the challenge data;

9 an authentication unit operable to perform an
10 authentication of the received signature data based on the
11 registered password and the challenge data; and

12 a content transmitting unit operable to, if the
13 authentication results in success, transmit an encrypted content
14 to the client apparatus, the encrypted content having been
15 encrypted in such a manner that the encrypted content can be
16 decrypted by the client apparatus.

1 3. The server apparatus of Claim 2 further comprising
2 a registering unit operable to register a password, which
3 is input from outside the server apparatus, with the holding
4 unit as the registered password.

1 4. The server apparatus of Claim 2 further comprising:

2 a distance judging unit operable to detect a communication
3 distance between the server apparatus and the client apparatus,
4 and judge whether the detected communication distance is within
5 a predetermined range of values; and

6 a registering unit operable to, if the distance judging

7 unit judges that the detected communication distance is within
8 the predetermined range of values, register a password, which
9 is transmitted from the client apparatus, with the holding unit
10 as the registered password.

1 5. The server apparatus of Claim 2, wherein
2 the holding unit holds a first password and a second
3 password that has a greater number of characters than the first
4 password, and
5 the authentication unit includes:
6 a distance detecting sub-unit operable to detect a
7 communication distance between the server apparatus and the
8 client apparatus;
9 a password selecting sub-unit operable to select the first
10 password if the detected communication distance is shorter than
11 a predetermined communication distance, and select the second
12 password if the detected communication distance is not shorter
13 than the predetermined communication distance; and
14 an authentication sub-unit operable to perform the
15 authentication of the received signature data based on the
16 challenge data and the selected password as the registered
17 password.

1 6. A client apparatus for receiving a content from a server
2 apparatus and reproducing the received content, comprising:
3 a receiving unit operable to receive challenge data from
4 the server apparatus;
5 a signature generating unit operable to generate signature

6 data based on the received challenge data and a first password;
7 a transmitting unit operable to transmit the generated
8 signature data to the server apparatus; and
9 a content receiving unit operable to, if an authentication
10 of the signature data results in success in the server apparatus,
11 receive an encrypted content from the server apparatus, the
12 encrypted content having been encrypted in such a manner that
13 the encrypted content can be decrypted by the client apparatus.

1 7. The client apparatus of Claim 6 further comprising
2 a password receiving unit operable to receive a password
3 which is input from outside, wherein
4 the transmitting unit transmits the received password to
5 the server apparatus, and
6 the server apparatus receives and stores the password as
7 a registered password.

1 8. The client apparatus of Claim 7 further comprising
2 a distance detecting unit operable to detect a
3 communication distance between the client apparatus and the
4 server apparatus, wherein
5 the transmitting unit transmits the received password to
6 the server apparatus if the detected communication distance is
7 shorter than a predetermined communication distance.

1 9. The client apparatus of Claim 6, wherein
2 a password of the client apparatus has been registered
3 with a server apparatus in advance,

4 the transmitting unit generates and transmits
5 authentication challenge data to the server apparatus before
6 the content receiving unit receives the encrypted content from
7 the server apparatus,

8 the content receiving unit receives, before receiving the
9 encrypted content, server signature data that is generated by
10 the server apparatus based on the transmitted authentication
11 challenge data and a first server password held by the server
12 apparatus,

13 the client apparatus further comprising:

14 a password holding unit operable to acquire a second server
15 password from the server apparatus with which the password of
16 the client apparatus has been registered, and hold the acquired
17 second server password; and

18 an authentication unit operable to perform an
19 authentication of the received server signature data based on
20 the authentication challenge data and the second server password,
21 wherein

22 the content receiving unit receives the encrypted content
23 from the server apparatus if the authentication of the server
24 signature data results in success.

1 10. The client apparatus of Claim 6 further comprising
2 a user authentication unit which includes:

3 a storage sub-unit operable to store, in advance, first
4 authentication data which is generated by extracting features
5 of first unique information that is a characteristic an
6 authorized user has uniquely as a living being;

7 an information receiving sub-unit operable to receive
8 second unique information input by a user, the second unique
9 information being a characteristic unique to the user as a living
10 being;

11 a feature extracting sub-unit operable to generate second
12 authentication data by extracting features of the second unique
13 information; and

14 a judging sub-unit operable to judge whether a rate of
15 match between the first authentication data and the second
16 authentication data exceeds a predetermined value, wherein
17 the signature generating unit generates the signature data
18 if the user authentication unit judges that the rate of match
19 exceeds the predetermined value.

1 11. An apparatus authentication system which comprises
2 a server apparatus and a client apparatus which perform a mutual
3 authentication when a content is transmitted from the server
4 apparatus to the client apparatus for use therein, wherein
5 the client apparatus includes:

6 a receiving unit operable to receive challenge data from
7 the server apparatus;

8 a signature generating unit operable to generate signature
9 data based on the received challenge data and authentication
10 data which is generated based on a characteristic of a user of
11 the client apparatus that the user has uniquely as a living being;
12 and

13 a transmitting unit operable to transmit the generated
14 signature data, and

15 the server apparatus includes:
16 a challenge data transmitting unit operable to generate
17 and transmit the challenge data;
18 a holding unit operable to hold, in advance, registered
19 data which is generated based on a characteristic that an
20 authorized user, who is authorized to use contents, has uniquely
21 as a living being;
22 a receiving unit operable to receive the signature data
23 from the client apparatus;
24 an authentication unit operable to perform an
25 authentication of the received signature data based on the
26 challenge data and the registered data; and
27 a content transmitting unit operable to, if the
28 authentication results in success, transmit an encrypted content
29 to the client apparatus, the encrypted content having been
30 encrypted in such a manner that the encrypted content can be
31 decrypted by the client apparatus.

1 12. A method for use in a server apparatus that transmits
2 a content to a client apparatus, wherein
3 the server apparatus holds a registered password,
4 the method comprising:
5 a challenge data transmitting step for generating and
6 transmitting challenge data;
7 a receiving step for receiving, from the client apparatus,
8 signature data generated based on a password and the challenge
9 data;
10 an authentication step for performing an authentication

11 of the received signature data based on the registered password
12 and the challenge data; and
13 a content transmitting step for, if the authentication
14 results in success, transmitting an encrypted content to the
15 client apparatus, the encrypted content having been encrypted
16 in such a manner that the encrypted content can be decrypted
17 by the client apparatus.

1 13. A program for use in a server apparatus that transmits
2 a content to a client apparatus, wherein
3 the server apparatus holds a registered password,
4 the program comprising:
5 a challenge data transmitting step for generating and
6 transmitting challenge data;
7 a receiving step for receiving, from the client apparatus,
8 signature data generated based on a password and the challenge
9 data;
10 an authentication step for performing an authentication
11 of the received signature data based on the registered password
12 and the challenge data; and
13 a content transmitting step for, if the authentication
14 results in success, transmitting an encrypted content to the
15 client apparatus, the encrypted content having been encrypted
16 in such a manner that the encrypted content can be decrypted
17 by the client apparatus.

1 14. A computer-readable recording medium which records
2 therein a program for use in a server apparatus that transmits

3 a content to a client apparatus, wherein
4 the server apparatus holds a registered password,
5 the program comprising:
6 a challenge data transmitting step for generating and
7 transmitting challenge data;
8 a receiving step for receiving, from the client apparatus,
9 signature data generated based on a password and the challenge
10 data;
11 an authentication step for performing an authentication
12 of the received signature data based on the registered password
13 and the challenge data; and
14 a content transmitting step for, if the authentication
15 results in success, transmitting an encrypted content to the
16 client apparatus, the encrypted content having been encrypted
17 in such a manner that the encrypted content can be decrypted
18 by the client apparatus.

1 15. A method for use in a client apparatus that receives
2 a content from a server apparatus and reproduces the received
3 content, the method comprising:
4 a receiving step for receiving challenge data from the
5 server apparatus;
6 a signature generating step for generating signature data
7 based on the received challenge data and a password;
8 a transmitting step for transmitting the generated
9 signature data to the server apparatus; and
10 a content receiving step for, if an authentication of the
11 signature data results in success in the server apparatus,

12 receiving an encrypted content from the server apparatus, the
13 encrypted content having been encrypted in such a manner that
14 the encrypted content can be decrypted by the client apparatus.

1 16. A program for use in a client apparatus that receives
2 a content from a server apparatus and reproduces the received
3 content, the program comprising:

4 a receiving step for receiving challenge data from the
5 server apparatus;

6 a signature generating step for generating signature data
7 based on the received challenge data and a password;

8 a transmitting step for transmitting the generated
9 signature data to the server apparatus; and

10 a content receiving step for, if an authentication of the
11 signature data results in success in the server apparatus,
12 receiving an encrypted content from the server apparatus, the
13 encrypted content having been encrypted in such a manner that
14 the encrypted content can be decrypted by the client apparatus.

1 17. A computer-readable recording medium which records
2 therein a program for use in a client apparatus that receives
3 a content from a server apparatus and reproduces the received
4 content, the program comprising:

5 a receiving step for receiving challenge data from the
6 server apparatus;

7 a signature generating step for generating signature data
8 based on the received challenge data and a password;

9 a transmitting step for transmitting the generated

10 signature data to the server apparatus; and
11 a content receiving step for, if an authentication of the
12 signature data results in success in the server apparatus,
13 receiving an encrypted content from the server apparatus, the
14 encrypted content having been encrypted in such a manner that
15 the encrypted content can be decrypted by the client apparatus.